

# Army electronic warfare:

## *A force multiplier or an electronic warfare Maginot Line?*

*The major fallacy of the Army's electronic warfare program lies not in its doctrine but in its method of execution of that doctrine and in the training and evaluation of those individuals charged with manning our electronic warfare wall of protection.*

*by Capt. Steven Williams*

The nucleus of the Army's electronic warfare program is its doctrine. Broadly speaking, the Army's electronic warfare effort attempts to deny the enemy the use of the electromagnetic spectrum for the marshalling, command and control of his forces while protecting the electronic communications and control systems of friendly operations. The major fallacy of the Army's electronic warfare program lies not in its doctrine but in its method of execution of that doctrine and in the training and evaluation of those individuals charged with manning our electronic warfare wall of protection.

During World War II, the Army's ground forces wanted to devise a method to jam enemy tank radios. Three questions evolved from that adventure, and their solutions can be considered the foundation for the successful development and execution of any electronic warfare program. They were: Who should coordinate and control the entire activity of monitoring

and jamming in various situations, as this or that arm might desire, according to this or that tactical exigency? Is it more valuable to listen to the enemy's signals for the intelligence gained or to jam them for some immediate tactical advantage in combat? Must not the control and assignment of frequencies be placed in the strong hands of an omnipotent and omniscient authority? The basic fighting unit of the Army is the infantry battalion. However, the Army decided with the formation of the first Communication Electronic Warfare Intelligence (CENI) battalion at Fort Hood, Texas, in 1976, that all questions pertaining to the execution of the Army's electronic warfare doctrine could be best answered by the omnipotent authority and the black box solutions.

The omnipotent authority solution grew out of the belief that only those individuals blessed with knowledge of

the big picture can effectively execute a viable electronic warfare response against a hostile adversary. This concept evolved from the recognition that electronic warfare was linked not only to tactical combat but to combat intelligence. Since radio intelligence is derived from the monitoring of enemy transmissions, one could not have individual commanders deciding for themselves to jam or to disrupt enemy command and control networks in order to achieve a local tactical advantage. The omnipotent authority, therefore, was the responsible individual who could provide the means with which to address problems of compartmentations. For this role Theater Army Intelligence Command (TAIC) was created.

The omnipotent authority solution is based on sound logic, but so were the solutions that lead to the building of the Mareth Line in Tunisia, the Gustus Line in southern Italy and the Maginot Line in France. Each of these fixed defensive systems was thought to be

***The omnipotent authority solution grew out of the belief that only those individuals blessed with knowledge of the big picture can effectively execute a viable electronic warfare response against a hostile adversary.***

force multipliers, but each fell victim to the tactic of swiftly moving armored columns. The Army's electronic warfare program will also fail if the following shortcomings of the omnipotent authority solution are not recognized and corrected.

The first major shortcoming of this solution is that it robs the local commander of an important source of intelligence pertaining to the battle plans and battle formations of the enemy with whom he is in direct conflict. This solution indirectly takes the local commander out of the flow of real time intelligence obtained by the electronic warfare specialist, who may be collocated and even assigned to him, but who is receiving operational guidance from TAIC headquarters. Since the electronic warfare specialist does not report directly to the local commander, he is more likely to be interested in collecting data pertaining to the concerns of the TAIC headquarters rather than of the local commander who is in imminent danger of direct contact with a hostile force.

The second major drawback of this concept is that it gives the decision to employ electronic support measures (ESM), such as directional finding and electronic countermeasures (ECM) such as the destruction of hostile transmitters, to the TAIC headquarters. This decision all but directs the development of ESM and ECM weapons and tactics along the needs or projected needs of the TAIC headquarters.

The combination of these two fallacies in the omnipotent authority solution not only forces the local commander to obtain the bulk of his electronic intelligence information by means of

the "TAIC Filter Down Method," but it also leaves him little or no means to conduct an offensive electronic warfare counteraction against the command and control network of those enemy tanks attacking his perimeter. He is only capable of employing passive electronic counter countermeasures to protect his own command and control networks which were found to be ineffective in World War I, World War II, Vietnam and during the 1973 Arab-Israel War. This assumption is based on the fact that the Soviet electronic warfare doctrine advocates the destruction or neutralization of NATO's command and control networks by utilizing jamming and physical destruction. The primary means of communications within the infantry battalion is the AN/PRC-77 and the VRC-12 radio series. It is estimated that the Warsaw Pact forces would be able to intercept, jam or destroy, transmissions by the AN/PRC-77 platoon radios 60 percent of the time within a ten-kilometer radius while the VRC-12 series radios, which are primary used for the battalion's command and control network, could be intercepted or neutralized almost 100 percent of the time.

***Washington's Army ran on its stomach Patton's Army ran on its gasoline supply today's volunteer Army runs on its FM radios.***

The second part of the Army's answer to how to execute its electronic warfare doctrine is the black box solution. Washington's Army ran on its stomach. Patton's Army ran on its gasoline supply, today's volunteer Army runs on its FM radios. Although the Army has a much greater dependency on its radios in order to accomplish its mission than the Warsaw nations, it possesses a far lesser capability to protect and utilize them in combat against a highly technical enemy such as the Soviet Union. A number of new sophisticated and expensive electronic warfare systems have been developed and are presently in various stages of

testing and development. Systems such as the AN/ALQ-151, long-range airborne interception and jamming system which will be carried in the Blackhawk utility helicopter; the AN/MLQ-34 (Tac-Jam), a tactical communications jammer; and various expendable jammers deliverable by artillery shell will add a great deal of reinforcement to our existing electronic warfare defensive wall.

However, the probability of these systems being any more effective than the electronic ground sensors employed along the Ho Chi Minh Trail during the Vietnam War is very remote. The reason for this pessimistic prediction of the effectiveness of these future systems is that the Army has yet to develop the tactics and operational concepts under which these systems are to be employed in support of combat operations. In order for these systems to become force multipliers, there must be a plan to integrate them directly into the combined arms concepts so that they may be readily utilized by the field commander in order for him to effectively engage and defeat the forces of the Warsaw Pact. During the short, violent but continuous conflict which the next war in Europe is destined to become, there will be little time to develop methods and techniques for the integration of new, untried electronic equipment into existing battle tactics and formations.

The Trident submarine fleet, the MX missile and the Army's electronic warfare program have one major point of interest in common: none of them has ever been battle tested. How successful the Army's electronic warfare program can be executed in an actual conflict can only be estimated by how well the men and women charged with the execution of this program perform during peacetime training and evaluation exercises. Therefore, the anticipated performance of these men and women in battle will be a direct result of the training — or lack of training — they receive during peacetime. It is ironic that the American Army, which prides itself on its peacetime training programs has never been able to successfully engage a hostile adversary without a crash retraining program at the outset of any armed conflict. "We must

***It is ironic that the American Army which prides its self on its peacetime training programs, has never been able to successfully engage a hostile adversary without a crash retraining program at the outset of any armed conflict.***

train in peace as we expect to act in war. We must learn today how to utilize our intelligence security and electronic warfare assets." This statement by Maj. Gen. William Rolya defines the basic problem with our electronic warfare training program. We do not train our communicators in peacetime as we expect them to act in a direct confrontation with the Warsaw Pact. Training can be divided into two distinct parts: first, teaching the communicator his job skills and evaluating how well he has learned those skills, and second, teaching the communicator his job and evaluating how well he has learned his job. The Army's ability to train communicators who can communicate in a hostile electronic environment is becoming a matter of grave concern. For example, in accordance with the omnipotent authority solution, infantry battalion commanders are only allowed to employ passive electronic counter-countermeasures against hostile transmitters in order to protect their communication command and control networks. It is well known that continuous wave (CW) is the best means of maintaining critical battlefield transmissions while being effectively jammed. However, this becomes extremely difficult when less than 20 percent of all Army communicators receive training in CW techniques. Whenever electronic warfare play is integrated into field training exercises, it usually works all too well, crippling or shutting down communications necessary to the completion of other aspects of the exercise.

The following conclusions can be drawn as a result of my analysis of the Army's electronic warfare program.

Everyone — from the front line soldier to the chairman of the Joint Chiefs of Staff — is aware of the growing threat that the Warsaw Pact poses to the radio command and control networks of our combat units.

Our response to this threat has been and continues to be an ineffective and incomplete electronic warfare command and control hierarchy, to which we have given expensive and untested weapons, for which we have not perfected the methods nor the procedures of integrating into our combined arms concept of battle.

This lack of a clear direction for the execution of our electronic warfare doctrine, coupled with a lack of trained

***The Army's ability to train communicators who can communicate in a hostile electronic environment is becoming a matter of grave concern.***

communicators in electronic warfare techniques, renders our entire electronic warfare program little more than a modern day French Maginot Line.

As a qualified electronic warfare specialist, I offer the following recommendations of actions in order to transform this modern day Maginot Line into a credible force multiplier.

The Army must recognize that the Soviet Union and its allies are capable of projecting as much fire power as deemed necessary to destroy our combat units. This massive capability is augmented by a highly effective and rapidly increasing electronic warfare offensive weapon system. During World War II it was generally agreed by friend and foe alike, that it was far more profitable to intercept each other's radio signals and analyze them for their intelligence value than to destroy them. However, with the development of modern encryption devices and the dependency of radios for command and control of fast moving battle formations, this gentleman's agreement is no longer valid. We must, therefore, recognize and prepare our forces to fight two

battles simultaneously in any future conflict. A battle for control of the land, and a battle for control of the airways. We must resign ourselves to the fact that control of either of these two areas of contention by the enemy will result in our certain defeat on the battlefield.

We must recognize that the electronic warfare battle has to be fought and won on two distinct levels. The individual unit level and the omnipotent authority level. Each individual unit from the infantry battalion upward must be equipped with the necessary electronic equipment and trained personnel to protect its own command and control network while denying the enemy with whom it is engaged the use of the electromagnetic spectrum. This can be accomplished in two ways: first, developing portable directional finding equipment, such as the SCR-504, hand-carried directional finder used in World War II. Equipment developed along this principle would give the infantry battalion the means of locating and possibly neutralizing hostile enemy jammers and transmitters located within its area of operation. Second, training our communicators to operate in a hostile electronic environment. This means instructions in the transmission and reception of CW transmissions must become a key building block in the development and training of our future and present radio operators.

We must place the horse before the cart in the development of our electronic warfare support equipment. We must: identify the threat, decide on the best solution that will enable us to eliminate or neutralize the threat, decide on what level the neutralization of the threat can best be accomplished, decide how to integrate our solution into our combined arms concept of battle, and develop and evaluate the equipment with which to accomplish the desired solution.

***The Army must recognize that the Soviet Union and its allies are capable of projecting as much fire power as deemed necessary to destroy our combat units.***

***We must recognize and prepare our forces to fight two battles simultaneously in any future conflict. A battle for control of the land and a battle for control of the airways.***

In sum, the major fallacy of the Army's electronic warfare program lies not in its doctrine but in its method of execution of that doctrine and in the training and evaluation of those individuals charged with manning our electronic warfare wall of protection. We must accept our enemy as the proficient, highly technical, battle worthy adversary that he is. Our enemy knows that a hard hitting, offensive action spearheaded by rapidly moving armor columns backed by artillery directed toward our communication command and control networks can neutralize or destroy any opposition sent against him. We must take whatever action necessary to develop a credible electronic warfare counterforce in order to protect our command and control networks. For as surely as German armor outflanked the France's Maginot Line in World War II and drove on to Paris, we may one day find our present electronic warfare defenses neutralized by fast moving Russian armor.

***We must accept our enemy as the proficient, highly technical battle worthy adversary that he is.***

#### *Glossary*

*Electronic Counter-Countermeasures (ECCM).* Protection of essential communications surveillance and target acquisition devices from interception, deception, jamming, location, and physical destruction by the enemy.

*Electronic Warfare Support Measures (ESM).* Search, intercept, identify, and locate emitters so that current and intended enemy actions can be determined.

*Electronic Countermeasures (ECM).* Prevent or effectively reduce the enemy's ability to use his communications, surveillance, and target acquisition devices (by jamming), or deceive the enemy so that he reacts to your best advantage (through imitative electronic deception).

*Continuous Wave (CW).* In this paper the term CW stands for manual morse.

#### **Bibliography**

Campen, Alan D., Col., USAF (Ret.). "Electronics—Just Another Element of Warfare," *Signal*, April 1981.

Commandant, U.S. Army Signal School. "Electronic Warfare: Tactics of Defense," (FM 32-30).

Ludvigsen, Eric C. "Conflict In the Ether: Delay, Destroy," *Signal*, June 1982.

Rolya, William I., Maj. Gen., USA. "Intelligence, Security and Electronic Warfare," *Signal*, March 1978.

Thomas, George Raynon and Harris, Dixie R. *United States Army in World War II, The Signal Corps: The Outcome (mid 1943-1945).*

*Capt. Steven Williams recently returned from Camp Long, Korea, where he was Signal Officer for the Combat Support Coordination Team #1. He is currently in Airborne School at Ft. Benning, Georgia. When he completes his training there, he will be assigned to the 18th Airborne at Ft. Bragg, North Carolina. He holds a B.S. in electrical engineering from Tuskegee Institute, Tuskegee, Alabama.*